Department of Commerce • National Oceanic & Atmospheric Administration • National Weather Service

NATIONAL WEATHER SERVICE INSTRUCTION 60-703

November 14, 2003

Information Technology
IT Security

Operational Controls

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W. Martin **Certified by:** B. West
Type of Issuance: Initial

SUMMARY OF REVISIONS:

Signed by Barry C. West 10/31/03
Barry C. West Date
Chief Information Officer

Table of Contents

1 Introduction. Operational controls address security methods that focus on mechanisms that are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). The types of control measures applied must be consistent with the environment and business requirements of the system and the need for protection of NWS Major Application or General Support systems. NWS IT Systems will ensure implementation in accordance with Federal regulations, DOC and NOAA policies, procedures, and guidance for the following operational controls:

Personnel Security
Physical and Environmental Protection
Production, Input/Output Controls
Contingency/Disaster Recovery Planning
Hardware and System/Application Software Maintenance Controls
Data Integrity/Validation Controls
Documentation

Security Awareness and Training

2 Definitions.

2.1 Classified and Unclassified Systems. A system is considered “classified” if it is used to electronically process, store, or transmit classified data. IT security requirements apply equally to classified and unclassified systems, but the rigor with which controls are implemented is greater for classified systems commensurate with the higher risk associated with classified data.

2.2 General Support System. According to National Institute of Standards and Technology Special Publication 800-18, a General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

2.3 Major Application. According to National Institute of Standards and Technology Special Publication 800-18, a Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

3 Personnel Security. The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impacts due to the well-intentioned actions of individuals authorized to use or maintain a system. Personnel security controls and procedures will be employed commensurate with risk of harm resulting from loss or damage to business or processes if compromised. The following controls will be used:

3.1 Positions will be reviewed for sensitivity level

3.2 Background screening will be performed as appropriate

3.3 Access to NWS IT Systems will not be granted to new employees or contractors prior to the completion of personnel screening (i.e., background) and awareness training

3.4 User access will be restricted to least privilege, (e.g., read, write, execute, delete) necessary to perform the task

3.5 Critical functions (e.g., ISSO, N/SA, etc.) when possible, will be divided among different individuals (separation of duties)

3.6 Procedures will be established for requesting, establishing, issuing, and closing user accounts (to include in-processing and out-processing check-lists) including procedures for friendly and unfriendly account termination

3.7 Mechanisms will be applied for holding users responsible for their actions

4 Physical and Environmental Protection. Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. Physical and environmental controls will be employed where required to ensure adequate protection of facilities, support facilities and systems. Controls to be considered include:

4.1 Fire Detection Devices

4.2 Cipher Locks

4.3 Uninterruptible Power Source (UPS)

4.4 Biometric Access Devices

4.5 Video Cameras

4.6 Alarms

4.7 Security Containers for Mobile and Lap Computers

4.8 Perimeter Fence

5 Production, Input/Output Controls. These are controls which support the operations of an application. NWS IT system owners will provide production input/output controls as required to ensure the level and posture of security for systems and applications are adequate. Controls may include:

5.1 A help desk or group that offers advice

5.2 Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information

5.3 Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.

5.4 Audit trails for receipt of sensitive inputs/outputs

5.5 Procedures for restricting access to output products

5.6 Procedures and controls used for transporting or mailing media or printed output

5.7 Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)

5.8 External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)

5.9 Audit trails for inventory management

5.10 Media storage vault or library with physical and/or environmental protection controls/procedures

5.11 Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)

5.12 Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse

5.13 Procedures for shredding or destroying hardcopy media when no longer required

6 Contingency/Disaster Recovery Procedures. All NWS IT systems will have plans or procedures to ensure the continuity of essential functions. These procedures will permit the organization to continue essential functions if IT support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) will be coordinated with the backup, contingency, and recovery plans of other NWS IT Systems, including networks affected by such failures. Plans and procedures will include:

6.1 Any agreements for backup processing
6.2 Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)

6.3 Location of stored backups and generations of backup

6.4 Procedures for testing contingency/disaster recovery at least annually

6.5 Procedures for training in roles and responsibilities relative to the emergency, disaster, and contingency plans

7 Hardware and System/Application Software Maintenance Controls. These controls are used to monitor the installation of, and updates to, application software and hardware to ensure the IT System functions as expected and that a historical record is maintained of changes. Hardware and system/application software maintenance controls will be applied to NWS IT Systems which ensure that only authorized software and or hardware is installed on systems. Such controls will include a software configuration approval process for modifications which requires that changes be documented. Controls to be used where applicable are:

7.1 Restriction/controls on those who perform maintenance and repair activities

7.2 Special procedures to perform emergency repair and maintenance

7.3 Procedures for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site)

7.4 Procedures for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements

7.5 Version control that allows association of system components with appropriate system version

7.6 Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production

7.7 Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software

7.8 Change identification, approval, and documentation procedures

7.9 Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes

7.10 Procedures to ensure live and production systems are not inadvertently used for test data
7.11 Adherence to organizational policies against illegal use of copyrighted software or shareware

8 Data Integrity/Validation Controls. Data integrity controls are used to protect data from accidental or malicious alteration and destruction. These controls provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements. NWS IT Systems will employ data integrity/validation controls as required to ensure a high level of integrity for operational products and data. Such controls will ensure adequate levels integrity for all other data consistent with risk associated with an integrity compromise. Controls to be applied as required by DOC, NOAA and NWS policies, procedures, and guidelines are:

8.1 Virus detection and elimination software

8.2 Reconciliation routines used by the system, e.g., checksums, hash totals, record counts

8.3 Integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions

8.4 Intrusion detection tools

8.5 System performance monitoring to analyze system performance logs in real time

8.6 Regularly scheduled penetration testing

8.7 E-mail message authentication/secure handling, e.g., PKI, digital signatures, encryption

9 Documentation. Documentation is a security control explaining how software and hardware will be used. It formalizes security and operational procedures specific to the system. Documentation for NWS IT Systems will include descriptions of the hardware and software, policies, standards, and procedures and will document approvals related to IT security for the application and the support system(s) on which it is processed. The system documentation will include backup and contingency plans as well as descriptions of user and operator procedures. Documentation will include:

9.1 Vendor documentation of hardware/software

9.2 Functional requirements or specifications

9.3 Security plan

9.4 Program manuals

9.5 Test results documents

9.6 Standard operating procedures

9.7 Emergency procedures

9.8 Contingency plans

9.9 User rules/procedures

9.10 Risk assessment

9.11 Accreditation/authorization to operate

9.12 Verification reviews/site inspections

10 Incident Response Capability. A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or

threatened breach of these mechanisms. When faced with an incident, the organization will respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. NOAA provides incident response for the NWS through the NOAA Computer Incident Response Team (N-CIRT). Each incident will be handled on a case by case basis, depending on the nature and severity. For all security incidents, the ISSO will provide an IT security incident report in accordance with NOAA guidance at https://www.csp.noaa.gov.

11 Security Awareness and Training. DOC, NOAA and NWS security policy, procedures and guidelines require the NWS IT Security Program to include an IT Security Awareness, Training, and Education component that applies to all employees (federal and contractor) as well as remote researchers and collaborators and temporary guests. NWS must coordinate Security Awareness training and each user of an NWS IT system must be trained before being granted permanent access to the system. Policy requires each user engage in annual refresher training to sustain such access. The rigor of the training may vary depending on the risk of harm posed by the user – for example, a guest for two days may be provided a document of the system rules to sign acknowledging understanding and acceptance, whereas a three-month summer intern may be required to complete a Web-based training course. Access provided to members of the public must be constrained by controls in the applications through which access is allowed, and awareness of such controls be made available to members of the public. System specific security awareness and training programs will identify requirements for and provide training to network and system administrators, security officers and focal points, and managers commensurate to the duties assigned and require:

11.1 Compliance with DOC, NOAA, and NWS awareness programs to include completion of the web based NOAA awareness training course

11.2 Documentation of the type and frequency of system security training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)

11.3 Procedures for assuring that employees and contractor personnel have been provided and completed adequate training